PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L

A2

(11) International Publication Number: **WO 98/25373**

(43) International Publication Date: 11 June 1998 (11.06.98)

(21) International Application Number: PCT/US97/21356

(22) International Filing Date: 21 November 1997 (21.11.97)

(30) Priority Data:
60/031,424 21 November 1996 (21.11.96) US

(71) Applicant: INTELLECTUAL PROTOCOLS, L.L.C. [US/US]; 271 Treetop Circle, Nanuet, NY 10954 (US).

(72) Inventor: GLOGAU, Jordan, J.; 271 Treetop Circle, Nanuet, NY 10954 (US).

(74) Agent: SHAPIRO, Stuart, B.; Epstein , Edell & Retzer, Suite 400, 1901 Research Boulevard, Rockville, MD 20850 (US).

(81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: WEB SITE COPY PROTECTION SYSTEM AND METHOD

(57) Abstract

A copy protection system and method protect web sites and other works in computer readable form from unauthorized access and/or reproduction. In particular, the copy protection system examines a web site or other work in computer readable form to ascertain the web site structure and individual web site components. A web site owner selects identified web site components for protection and provides a protection level for those components. An end–user attempting to access protected web site components is directed to obtain a license wherein the copy protection system displays licensing terms to the end–user and administers a test relating to the licensing terms. Upon passing the test, the copy protection system grants the end–user a license and enables the end–user to download software that facilitates access and/or reproduction of the protected web site components. If the end–user does not obtain a license, the copy protection system permits the end–user to access and/or reproduce only unprotected web site components.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Paso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

PATENT APPLICATION

Title: Web Site Copy Protection System and Method

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from U.S. Provisional Patent Application Serial No. 60/031,424, entitled "Web Site Copy Protection System and Method", filed November 21, 1996. The disclosure of that provisional patent application is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention pertains to computer systems for protecting web sites or other works in computer readable form from unauthorized access and/or reproduction. In particular, the present invention is directed toward a computer system for enabling only licensed end-users to access protected material of an internet web site wherein the computer system may automatically present licensing terms to an unlicensed end-user and grant a license to the unlicensed end-user upon the unlicensed end-user's acceptance of the licensing terms.

2. Discussion of the State of the Art

Briefly, the growth of the World Wide Web (herein referred to as the Web) has been an unprecedented event in the history of computers and telecommunications. Internet traffic has increased from five terabytes (i.e., tera represents 10^{12} or one trillion) a day in the fall of 1994 to 250 terabytes a day in the summer of 1996. Further, personal computer sales will surpass television sales in the United States for the first time in 1996, while data telecommunications traffic will similarly overtake voice traffic. Most of these events can be attributed to the growth of the Internet and the Web.

Although the Web is a wonderful environment to transact business and disseminate information, there are a number of disadvantages that make it unattractive. Specifically, there is typically no provision on the Internet, and the Web in particular, to protect material from being indiscriminately copied and reproduced with impunity. Since the act of transferring files from one computer to another via the Internet involves essentially exact reproduction of the material, it is difficult to protect that material from unauthorized use. Although copyright protection may assist in deterring the unauthorized reproduction of material, the computer industry has been restricted in enforcing copyrights in certain situations; for example, it is lawful to reproduce material for purposes of back-ups (i.e., saving the material in case of data loss due to computer or memory failure). Further, the Internet enlarges the protection problem because of its worldwide nature and the fact that the Internet is designed based in part on the concept of free reproduction. Currently, the software industry believes that the ratio of unauthorized reproductions to authorized reproductions is approximately five to one.

Typically, a web site includes various types of works, such as text, images, art work, audio and video. These works are generally eligible for copyright registration with the appropriate authority (e.g., the Copyright Office) wherein the copyright for the works automatically exists upon their creation, and registration of the work with the appropriate authority (e.g., the Copyright Office) enables the copyright or web site owner to enforce the copyright. Although each web site work, and the entire web site itself, may be protected by copyright, procedures are typically required to assist in enforcing the copyright. For example, industry has utilized copy protection techniques wherein these techniques prohibit unauthorized reproduction of protected material, but do not provide additional legal protection (e.g., a contract or license) to enhance the copyright owners' enforcement of their rights. However, the existence of a license does not guarantee

absolute protection since certain licenses, such as shrink wrap licenses (i.e., licenses printed on packaging or displayed by software), may be unenforceable due to the fact that the license is often ignored and not read by parties utilizing the protected material. Therefore, the present invention is directed toward providing enhanced protection of a web site or other work in computer readable form against unauthorized reproductions. In particular, the present invention permits only licensed end-users to access protected web site material, automatically presents licensing terms to an unlicensed end-user and grants a license to the unlicensed end-user upon the unlicensed end-user's acceptance of the licensing terms. Further, the present invention provides a copying utility to licensed end-users for selective reproduction of protected web site material. The copying utility functions in tandem with web site protection utilities as described below to ensure that only appropriate web site material is accessed by licensed end-users, thereby protecting a web site from unauthorized or unlicensed access and/or reproductions.

OBJECTS AND SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to selectively protect components of a web site or other work in computer readable form from unauthorized access and/or reproduction.

It is another object of the present invention to selectively grant licenses for authorized access and/or reproduction of protected components of a web site or other work in computer readable form.

Yet another object of the present invention is to ensure comprehension and acceptance of license agreement terms by unlicensed end-users such that licenses may be

granted to authorize the unlicensed end-users to access and/or reproduce protected components of a web site or other work in computer readable form.

The aforesaid objects are achieved individually and in combination, and it is not intended that the present invention be construed as requiring two or more of the objects to be combined unless expressly required by the claims attached hereto.

According to the present invention, a copy protection system selectively protects components of a web site or other work in computer readable form by limiting access and/or reproduction of protected components to licensed or authorized end-users. Specifically, the copy protection system includes a copy protection system server (e.g., a computer system that services client requests) having site examination server software and licensing software, and end-user computer systems each associated with a corresponding end-user. The copy protection system server, via site examination server software, identifies web site components and provides protection to identified web site components selected by a web site owner, while licensing software enables the copy protection system server to grant licenses that authorize end-users to access and/or reproduce web site components protected by the copy protection system. A licensed end-user may download site copying software to an associated end-user computer system from the copy protection system server wherein the end-user computer system, via site copying software, interacts with the copy protection system server to enable the licensed end-user to access and/or reproduce protected web site components.

Initially, the web site owner enters information relating to a web site the owner desires to protect (e.g., the uniform resource locator (URL) of the web site) into a copy protection system web site residing on the copy protection system server. The information relating to the owner web site may be entered into the copy protection system web site via

an internet browser residing on a web site owner computer system. The copy protection system server subsequently retrieves files associated with the owner web site based on the entered information and examines that web site to ascertain the web site structure and to identify individual web site components. The web site owner, via the copy protection system web site and server, selects identified web site components for copy protection and designates a level of protection desired for each selected web site component. Special tags or codes are inserted by the copy protection system server within web site files associated with the owner web site to indicate the web site components selected for protection. A permission table is constructed for each web site protected by the copy protection system to store the protection status of web site components and authorized access information (e.g., codes indicating whether or not an end-user possesses a license). The permission table is utilized by the copy protection system to determine whether or not an end-user possesses a license authorizing the end-user to access and/or reproduce a protected web site.

In response to an attempt by an unlicensed end-user to access a protected web site, the unlicensed end-user is linked (i.e., transferred) to the copy protection system web site wherein the unlicensed end-user may obtain a license for authorized access and/or reproduction of protected web site components. Specifically, the copy protection system server displays licensing agreement terms to the unlicensed end-user wherein clarification pages relating to and explaining the license agreement terms may further be displayed in response to an indication that the unlicensed end-user does not understand a displayed licensing agreement term. Subsequent to reviewing the license agreement terms and/or associated clarification pages, the unlicensed end-user must pass an on-line test or quiz administered by the copy protection system server in order to obtain the license. The copy protection system server examines test answers and grants the license to the unlicensed

end-user in response to a correct answer for each test question. However, if test questions are answered incorrectly, the copy protection system server displays clarification pages for licensing agreement terms associated with each incorrectly answered test question. After the unlicensed end-user reviews the license agreement terms and clarification pages relating to incorrectly answered test questions, a modified on-line test or quiz is administered to the unlicensed end-user by the copy protection system server. The unlicensed end-user must pass the modified test by correctly answering each test question in order to obtain the license. Alternatively, the test or quiz may be administered via fax, telephone, mail or in any other suitable manner wherein test answers may be graded by an external device (e.g., character or other type of reader).

Upon granting a license to an unlicensed end-user, the copy protection system server modifies or places a special code within a cookie file (i.e, a file containing end-user information associated with an end-user internet browser) associated with the end-user to indicate that the end-user possesses a license. Further, site copying software may be downloaded by a licensed end-user to an associated end-user computer system from the copy protection system server to enable the end-user computer system to access and/or reproduce protected web site components. The copy protection system, via site copying software and site examination server software, verifies the information contained within the end-user cookie file against the information contained within the permission table associated with the protected web site to enable the licensed end-user to access and/or reproduce protected web site components in accordance with access privileges granted to the end-user by the license. If the end-user does not obtain a license, the copy protection system enables the unlicensed end-user to access only unprotected web site components. Thus, the copy protection system enables web site owners to selectively determine web site

components to be accessed and/or reproduced, thereby preventing unauthorized reproduction of those web site components.

The above and still further objects, features and advantages of the present invention will become apparent upon consideration of the following detailed description of a specific embodiment thereof, particularly when taken in conjunction with the accompanying drawings wherein like reference numerals in the various figures are utilized to designate like components.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a view in perspective of an exemplary computer system employed by the present invention.

Fig. 2 is a functional block diagram of protected web sites, permission tables and site copying software illustrating the manner in which permission tables are utilized to determine end-user access rights for protected web site material according to the present invention.

Fig. 3 is a block diagram of TCP/IP protocol layers.

Fig. 4 is a block diagram of an exemplary hierarchical structure of a web site.

Fig. 5 is an exemplary HTML file containing tags (i.e., web site formatting instructions) for generating a web site page.

Figs. 6 - 10 comprise a procedural flow chart illustrating the manner in which the copy protection computer system grants licenses to end-users and enables only licensed end-users to access protected web site components according to the present invention.

Fig. 11 is a system flow chart illustrating the manner in which the copy protection computer system determines that an end-user is authorized to access protected web sites according to the present invention.

Fig. 12 is a flow diagram illustrating the manner in which the copy protection computer system verifies end-user understanding of license terms before granting a license according to the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

An exemplary computer system employed by the present invention for implementing web site copy protection is illustrated in Fig. 1. Specifically, computer system 61 is a conventional IBM-compatible or other type of personal computer preferably equipped with a monitor 63, base 65 (i.e., including the processor, memories, and internal or external communication devices or modems), keyboard 69 and mouse 67. The copy protection system (CPS) typically includes a plurality of computer systems 61 (e.g., a copy protection system server or a third party server, a web site owner computer system and an end-user computer system), each computer system including a different portion of copy protection software. Specifically, the copy protection system utilizes software that includes independent but related components, namely site examination server software, site copying software and licensing software. The site examination server software preferably resides on the copy protection system server (e.g., a computer system that services client requests) and ascertains the protected web site structure, while site copying software is typically downloaded from the copy protection system server onto an end-user computer system to facilitate selective copying of protected web site material as described below. The licensing software typically resides on the copy protection system server and grants end-

users licenses to access protected web site material as described below. Alternatively, site examination server software may reside on a computer system server of a third party possessing a license for site examination server software, or on a web site owner computer system (i.e., a client version of the site examination server software residing on the web site owner computer system). The site copying software enables selective reproduction of web site material and works in conjunction with the site examination server software similar in relation to a client-server application (i.e., an application where a computer system or server processes requests from several client or end-user computer systems). The site copying software is designed to function as a helper application or "plug-in" (i.e., software that extends the basic features of a software package and functions as though it is part of that package) to internet browsers, such as Netscape, Mosaic, Internet Explorer or other browser. However, the site copying software may also be a stand-alone program, or software developed by third parties having a license to develop such software. The site examination server software examines a web site and constructs a permission table to define access schemes for web site components based on web site owner preferences. Each protected web site is processed by the site examination server software to construct individual permission tables for use by the site copying software as illustrated in Fig. 2. The site copying software may be in the form of a stand-alone program 96, a "plug-in" 97 to an internet browser, or a third party copying utility 98. Specifically, the site examination server software constructs individual permission tables 95 for each protected web site 90, 92, 94. Each permission table typically includes information relating to end-users licensed for a respective web site and the protection afforded to the respective web site components. When an end-user visits a protected web site 90, 92, 94 and desires local copies of web site material, the site copying software 96 (e.g., a stand-alone version), 97 (e.g., a plug-in

version), or 98 (e.g., third party software) resident on the end-user computer system utilizes permission tables 95 to determine end-user access rights and corresponding web site components to copy to the end-user computer system based on the license and protection information contained in the table. When the end-user does not possess a license, permission tables 95 either permit access to only unprotected web site components, or totally deny access to the web site when all web site components are protected.

Each computer system may utilize any of the major platforms or operating systems, such as Windows, Macintosh, Unix or OS2. Further, the computer systems containing the site examination server software (e.g., the copy protection system server or third party server, or the web site owner computer system) and licensing software (e.g., the copy protection system server) preferably include at a minimum an Intel 80486 or compatible processor, eight megabytes of RAM, and sufficient disk storage (e.g., hard drive) to store at least ten megabytes of data and web browser software. The computer system containing the site copying software (e.g., the end-user computer system) is substantially similar to the computer system containing the site examining server software and licensing software described above except that the computer system containing the site copying software requires sufficient disk storage (i.e., hard drive) to store at least one megabyte of data and web browser software. Moreover, the end-user of the computer system containing the site copying software controls the allocation of disk storage used for local copies of protected web site material.

The copy protection system assists web site owners in protecting their web sites from unauthorized reproduction. The main system concept is to enable an end-user to locally reproduce web site material in a manner that is satisfactory to the web site owner. The copy protection system provides a special web site copying utility (i.e., the site

copying software described above) to the end-user for enabling the end-user to produce legitimate copies of web site material after the end-user agrees to be bound by a system generated license. The use of other copying facilities is generally outside the scope of the license and is prohibited unless specifically approved by the copy protection system provider. The following steps outline the manner in which web site material is protected.

1. Material on the web site is protected by copyright (i.e., upon creation of the material and preferably registered with the appropriate authority (e.g., the Copyright Office)).

2. A web site owner enters a web site into the copy protection system.

3. The web site is modified by the copy protection system (i.e., via the site examination server software described above) to permit web site access by authorized end-users.

4. An end-user attempts to access the protected web site.

4.1 The end-user is informed by the copy protection system (i.e., via the licensing software described above) of the terms and conditions for accessing the site and the fact that site access includes the use of copyrighted copying software (i.e., the site copying software described above) registered with the appropriate authority (e.g., the Copyright Office).

4.2 The end-user agrees to the terms and conditions of web site access and indicates acceptance of the terms either on-line, or by telephone, fax or mail.

4.3 The end-user downloads free copying software (e.g., the site copying software described above) to the end-user computer system.

4.4 The end-user accesses web site information.

5. An unauthorized end-user reproduces protected web site material.

5.1 The unauthorized end-user is discovered.

5.2 The unauthorized end-user is informed of the violation (e.g., copyright violation for reproducing copyrighted material).

5.3 The unauthorized end-user is informed of the terms and conditions for legitimate reproduction and use of the protected web site material.

5.3.1 The unauthorized end-user agrees to the terms and conditions for legitimate reproduction and use of the protected material.

5.3.2 The unauthorized end-user does not agree to the terms and conditions for legitimate reproduction and use of the protected material, and legal remedies are pursued.

Briefly, the Web is a Client-Server service (i.e., a service wherein a computer system or server processes requests from several client or end-user computers) that executes at the top of the Transmission Control/Internet protocol (TCP/IP) layers 100 as illustrated in Fig. 3. The protocol layers dictate the manner in which computers communicate with each other as described below. The TCP/IP layers are less complex than the standard IOS model (i.e., another standard layered protocol) and have become the worldwide standard for communications among different computer systems. Specifically, the Internet Protocol, Datalink, and Physical layers 66, 68, 70 are associated with the physical transfer of data across different media, such as modem, dedicated T1 (i.e., a communication scheme for digital transmission) or LAN (i.e., local area network), and the manner in which the different media handshake or communicate. Transport layer 64

includes a Hypertext Transport Protocol (HTTP) that enables the Web to request and send data from one computer to another, while Application level 62 includes a web browser (i.e., software that enables an end-user to traverse the Web), such as Netscape, Mosaic, Internet Explorer or other browser, residing on the client (i.e., end-user) system and a web server (i.e., software that enables the server to process client requests) residing on the server system. An end-user at a client system typically enters an internet address in the appropriate field on a web browser window to request or visit a particular internet web site. The entered address usually contains the prefix "http" and is forwarded to an internet service, namely Domain Name Service (DNS), wherein the service stores the computer address of the computer, typically a server, containing the requested site. The request is then sent to the server residing at the computer address and containing the requested site wherein the server downloads the site to the end-user computer via the Internet. The site is then displayed on the end-user computer screen using the client web browser.

The structure of a web site is based on the standard tree structure utilized by most major and conventional computer operating systems. A typical hierarchical structure 72 utilized in conventional computer operating systems and demonstrating the manner in which a majority of web sites are stored within those operating systems is illustrated in Fig. 4. A simple web site can consist of a single file, but generally a web site contains many files. Specifically, structure 72 includes a top level or root node 74 having subordinate nodes 76 (web site), 78 (programs) and 80 (E-mail (i.e., electronic mail)). Programs node 78 includes programs (e.g., common gateway interface (CGI) scripts that reside on the server and are initiated by the web browser via user input) utilized by the web site to perform various functions, such as animation, while E-mail node 80 typically contains information relating to the transmission and reception of electronic mail. Web site node

76 typically includes a subordinate node pertaining to a home page 82 with links to subsequent nodes or pages of information, such as company background 84, products 86 and order forms 88. These links are known as Hyperlinks and are a powerful utility of the Web enabling transference to various web pages. The links also enable return from company background, products, and order form pages 84, 86, 88 to the home page 82 (i.e., commonly referred to as the index since the home page enables transference to particular locations in the web site, such as the company background, products and order form pages) such that an end-user can easily restart traversal of the web site structure. Hyperlinks are not limited to transference among locations within one's own site, but can transfer an end-user to any other page residing on the Web. Hyperlinks are similar to references and/or footnotes encountered in written works except that the reference is available without having to leave the main body of the work. In terms of the Internet, the web is the main body with web pages being references and/or footnotes. Further, a web site may have Hyperlinks to other internet services, such as E-mail and File Transfer Protocol (FTP). FTP is typically utilized to transfer files and download software. In addition, a web site may include forms where an end-user enters information on a form and the web site interacts with the end-user via a CGI script described above or other programming protocols.

The web site files are written in accordance with a particular syntax that is central to the Web, namely the Hypertext Markup Language (HTML). HTML is a language constructed of text that has delimiter codes incorporated into the language to represent a procedural call. These procedural calls indicate the type of processing and/or arrangement for text, graphic and related objects that form the web site. In particular, HTML utilizes less than (i.e., "<") and greater than (i.e., ">") symbols as code delimiters with HTML instructions or tags placed between these two symbols (e.g., ⟨TITLE⟩). A small exemplary

HTML file showing different types of tags that indicate whether or not text is body matter, a heading or a title is illustrated in Fig. 5. Other tags include links, and calls to graphics, sound files and programs (e.g., CGI scripts). The tags enable the copy protection system to identify various objects within a web site that may require protection.

Web sites typically include a plurality of various media types that are generally each individually eligible for copyright registration. These media types commonly take the form of works listed, by way of example only, in Table II below. For example, graphic works are considered to be pictorial with copyright registration generally being accomplished via form VA, while text and tables are considered to be literary material with copyright registration generally being obtained via form TX. The various types of works shown in Table II are typically contained in files preferably having the designated file extensions (i.e., NA indicates that there is no designated extension or an extension is not applicable). A web site typically includes software that can process the files to attain the desired effect (e.g., sound, picture, etc.). The various web site works described below may each have their own separate copyright registration dependent upon their commercial value.

TABLE II

TYPE OF WORK	NAME	FILE EXTENSION	COPYRIGHT FORM REQUIRED FOR FILING
Text, Tables	HTML	htm or html	TX
Graphic	GIF	gif	VA
Photograph	JPEG	jpg or jpeg	VA
Audio	Wave	wav	SR
Digital Music	Midi	mid	PA
Audio Streaming	Real Audio	NA	PA
Multimedia	Shockwave	NA	PA
Program	Java	java	TX
Program (Forms)	CGI	cgi	TX
FTP (File Transfer)	NA	NA	TX
Computer Animation	NA	NA	VA

The copy protection system basically includes two phases that are performed in order to protect a web site. The first phase includes incorporating the web site into the copy protection system and providing site copying software to licensed end-users for facilitating reproduction of protected web site material. The second phase of the copy protection system enables only licensed end-users to access protected web site material. Initially, a web site for which protection is desired is configured in a certain manner to restrict access to particular web site components in accordance with web site owner preferences. Specifically, the copy protection system (i.e., via the site examination server software described above) performs an initial examination of the web site and identifies various web site components by media types or objects generally contained in Table II. A subsequent inquiry is performed for each component to obtain from the web site owner whether or not the component is to be protected, and the level of protection desired (e.g.,

the component level or distance from the root node within the web site hierarchical structure requiring protection wherein subsequent levels of web site components coupled to the higher level protected component are also protected). Generally, the web site owner visits the copy protection system web site via a web browser residing on the owner computer system wherein the owner is prompted for the address of the web site requiring protection. The owner subsequently enters the Uniform Resource Locator (URL, i.e., the web site internet address) for the web site into a dialog box or form to start the copy protection process. The site examination server software retrieves and examines the whole web site structure 72 (Fig. 4) including tags found in web site HTML files (Fig. 5) to identify various web site components. The HTML tags may indicate media types of, and usually indicate files containing, web site components (e.g., image files, sound files, etc.). The file extensions of web site media files may also indicate media types as described above, by way of example only, in Table II. Subsequently, a series of questions is presented to the web site owner in a dialog box, form or line prompts relating to inclusion and exclusion of web site components for copy protection. For example, certain graphics of a utility nature should be ignored and automatically excluded from copy protection by the system, such as bullets for bulleted lists and simple lines that are used as dividers on the screen. These utility graphics can be excluded based on either their size (e.g., number of bytes and/or length and width) and/or title. The site examination server software typically sets a protection flag (i.e., " Protection Tag" element of an HTML object data structure described below) in order to indicate web site components that are to be protected and the level of protection desired, while setting an ignore flag (i.e., "Ignore Flag" element of an HTML object data structure described below) to bypass web site components that are to be ignored. Further, the site copying software described above is made available for

downloading to end-user computer systems to enable end-users consenting to a license to copy protected web site material.

Once a web site is configured and the copying software is available for downloading as described above, end-users may attempt to visit a protected site. Upon visiting a protected site, the end-user is presented with terms and conditions for accessing protected web site material and using the site copying software. The end-user must agree to the terms and conditions prior to accessing the web site. However, one of the major problems with licensing software is ascertaining the end-user's understanding of the terms and conditions of the license. The copy protection system, via the licensing software, assists the end-user with comprehending the license terms by selectively displaying major license components with a clarifying explanation, and testing the end-user on license subject matter. The end-user endures this licensing procedure since each protected web site is licensed by substantially the same terms, thereby requiring the procedure to only be performed once to visit any protected site. The goal of the copy protection system is to ensure that end-users carefully read the license and understand the license terms. The terms basically include the right to use the site copying software when the end-user desires a local copy of web site material, however, the license terms must be upheld whether or not the end-user uses the site copying software to produce local copies. When the end-user desires local copies of protected web site material at a later date, the end-user simply returns to a protected web site to download the site copying software as described below.

The copy protection system (i.e., via the site examination server software) utilizes an overall data structure for the web site including a master list of HTML tags or objects encountered during examination of web site files. Each HTML object includes a record

having a component indicating whether or not that object is to be protected and the level of protection desired (i.e., the "Protection Tag" element). The HTML object further includes the object media type and other related information (e.g., file location, ignore flag, creation date, modification date, ownership, links, etc.). The HTML objects essentially decompose a web site into its smaller components since each web site component may require a different degree of protection, or no protection at all. Further, since large protected web site components may usually be decomposed into protected and unprotected web pages and/or files, a web site component that is an element of a larger protected web site component may be protected under the larger component protection and not need individual protection. For example, a newspaper may offer a top level headline web page for free viewing, however, detailed stories may only be available to end-users that subscribe to the newspaper. In order for the end-user to maintain local copies of stories on the end-user computer system, the end-user requires specialized software, similar to the site copying software described above, to copy stories to the end-user computer system.

Once an end-user is authorized to access protected web sites, the end-user computer system maintains a small End-User object (i.e., a small record) within a cookie file associated with a web browser on the end-user computer system. The cookie file is typically a simple ASCII file associated with internet browsers that contains end-user information (i.e., an End-User object described below having the user name and a code) wherein the file can be read or written by the copy protection system software (e.g., the site examination server software and the licensing software as described below) when the end-user attempts to access a protected site. Typically, the cookie file is examined when an end-user accesses a protected site to determine whether or not the end-user is entitled to access protected web site material. If the code is not present within the

cookie file, the user is directed to obtain a copy protection system license in order to access protected web site material. The code is basically an encrypted key that is associated with the user name contained within the permission tables described above.

In Object Oriented Programming (OOP), the data and data processing are stored as a single set of computer instructions. In other words, the data type and processing instructions are merged. This feature enables creation of Client-Server applications, such as the Web. The Gane/Sarson web site data structure outline for the web site, HTML and End-User objects is illustrated below.

Web Site Object
- HTML Object List

HTML Objects
- File Location
- Ignore Flag
- Types
  - Text
  - Artwork
  - Photograph
  - Database
  - Link
  - Program
    - Java Applet
    - Xactive
- Creation Date
- Modification Date
- Ownership
- Links (Internal)
  - To
  - From
- Protection Tag
  - Yes/No
    - Level

End-User Object/Cookie File on End-User's System
- Name
- Code (Encrypted Key)

A procedural flow chart showing the operation of, and the manner in which a web site is protected by, the copy protection system is illustrated in Figs. 6 - 10. Specifically, a web site owner initially determines at step 1 that information on the owner's web site

requires protection. The owner visits the copy protection system (CPS) web site at step 2 via the owner computer system web browser wherein the owner is presented (e.g., via licensing software resident on the copy protection system server containing the system web site) with terms for web site protection and conditions under which the copy protection system grants licenses to end-users for accessing a protected web site. When the owner agrees to the protection terms and end-user licensing conditions at step 3, the site examination server software loads the owner web site files at step 4, and examines the files at step 5 to decompose the web site into its smaller components or objects based on HTML tags within web site files as described above. An object table containing entries for web site objects is constructed by the site examination server software at step 6 from the web site examination, and preferably stored in computer memory or a commercially available or conventional database. The site examination server software may reside on the copy protection system server, a third party server containing the owner web site and licensing the site examination server software, or on the owner computer system in a client version. It is to be understood that the references to software performing functions as used herein actually refer to a computer system performing the functions under control of that software.

Once web site objects are identified, the site examination server software presents the owner with a series of inquiries to ascertain web site objects to be automatically excluded from protection or ignored as described above. The web site objects are examined via the site examination server software and each object that has not been excluded (i.e., the "Ignore Flag" element of the HTML object data structure described above is not set) is presented to the owner in an object loop (i.e., a series of computer instructions that are repeated for each object) to ascertain whether or not protection for that object is desired. Specifically, the object loop determines at step 7 whether or not each object has been processed. When objects have not been processed, the next object is

retrieved and the owner determines at step 8 whether or not the retrieved object requires protection. If the owner enters information (e.g., via keyboard, mouse or any other conventional input device) indicating that the object does not require protection, the protection flag (i.e., the "Protection Tag" element of the HTML object data structure described above) is not set as indicated at step 9. However, if the owner enters information indicating that the object requires protection, the owner subsequently enters the desired protection level (e.g., the object level or distance from the root node within the web site hierarchical structure requiring protection wherein subsequent levels of web site objects coupled to the higher level protected object are also protected) at step 10, and the protection flag (i.e., the "Protection Tag" element of the HTML object data structure described above) is set to indicate the level of protection required at step 11. The web site owner is able to protect different portions of the web site based on the web site hierarchical structure (Fig. 4) and the level of protection indicated for a particular web site object. After the protection status of the object has been designated, the next object is retrieved for processing at step 7.

Referring to Fig. 7, when the owner has entered protection preferences for each web site object, an access (i.e., permission) table indicating the protection status of each web site object is constructed by site examination server software at step 12, and preferably stored in a computer memory or commercially available or conventional database. The web site objects are examined in a second object loop within the site examination server software in order to inspect the web site objects and modify corresponding web site files (e.g., HTML files) associated with each protected object. Specifically, the second object loop determines at step 13 whether or not each web site object has been processed. When web site objects have not been processed, the next web site object is retrieved and its

protection flag (i.e., the "Protection Tag" element of the HTML object data structure described above) examined at step 14 to determine whether or not the object is to be protected. If the object requires protection, the corresponding portion of web site HTML files are modified by site examination server software at step 16 to enable limited access to that web site object. In particular, the web site is modified by embedding a special tag or code within web site HTML files associated with the protected web site object. The tag may comprise any characters or symbols that do not conflict with existing HTML tags or commands. The special tag indicates to site examination server software and site copying software particular objects that are protected, thereby controlling access to protected web site components. The special tags basically identify web site components within HTML web site files that should not be sent to unlicensed end-user computer systems for display on end-user web browsers or storage in the end-user computer system. If the web site object is not to be protected, web site files are not modified as indicated at step 15. After the object is processed, the next object is retrieved for processing at step 13.

Upon modifying web site files in accordance with web site object protection designations, the web site may handle access requests by end-users at step 43. Specifically, when an end-user visits a protected site via an end-user web browser, the site examination server software determines at step 44 whether or not the end-user has previously visited a protected site and obtained a license. This is automatically determined by examining the end-user cookie file in the end-user web browser as illustrated in Fig. 11. The cookie file includes the end-user name and code as described above wherein the code indicates the presence of an end-user license. Specifically, the end-user visits a protected web site 73 by requesting access via a web browser 77 residing on the end-user computer system. By way of example only, web site 73 resides on a third party server containing a licensed copy

of site examination server software. The site examination server software examines end-user cookie file 79 and special tags within HTML web site files being accessed. Subsequently, the site examination server software determines end-user access rights by inspecting the access (i.e., permission) table associated with web site 73 in a local end-user database 81 for the encryption key or code contained in the cookie file wherein the existence of the key in the database indicates the presence of a license. The site examination server software may alternatively consult the access table for web site 73 in end-user database 83 residing on the copy protection system server containing a copy protection system web site 75. However, since database 81 is local to the server containing site examination server software and web site 73, database 81 provides a faster overall access time than database 83. The databases may be implemented by any conventional or commercially available databases. The presence of an end-user license may also be indicated in various other manners, such as by use of a password, end-user name, information in a local file or other incorporated feature indicating the presence of a license. Further, site examination server software and web site 73 may reside on the copy protection system server, or on the owner computer system and function in substantially the same manner described above to determine end-user access rights for protected web site material.

Referring to Fig. 8, when an end-user visits a protected web site for the first time at step 17, the end-user is "linked" (i.e., transferred) from the protected web site to the copy protection system web site at step 21 where licensing software resident on the copy protection system server presents the end-user with licensing terms for access to the protected site at step 23. After viewing licensing terms, the end-user determines at step 24 the manner in which to further view and execute the proposed license agreement. The end-

user may execute the license as described below either on-line at step 18, or via fax, mail or telephone at steps 20, 22, 60, respectively.

The copy protection system obviates the problems of end-user comprehension of licenses described above via on-line execution at step 18. Specifically, each license section is typically presented to the end-user on a web page or form one section at a time. Once each license section has been presented, a license agreement summary is displayed emphasizing major license terms. Subsequently, a series of multiple choice questions relating to subject matter of the license is displayed for the end-user to answer. The licensing process should endure for five to ten minutes and is illustrated in Fig. 12. Specifically, an overview page 45 is initially displayed and includes the procedure for responding to questions, the complete agreement and a warning that failure to follow the procedure may cause the end-user to restart the licensing process. The warning further states that questions relating to main points of the license must be answered correctly in order to obtain a license. After the overview page, a first license section 46 is displayed for review. The end-user is prompted as to whether or not the end-user understands that license section. If the end-user enters information indicating that the end-user does not understand that section, a clarify page 50 is displayed containing supplemental information about the license section. Subsequent license sections 47, 48, 49, and corresponding clarification pages 51, 52, 53 are respectively individually displayed for review by the end-user in substantially the same manner described above for license section 46 and clarify page 50. After each license section has been reviewed by the end-user, a summary page 54 is displayed wherein the full license is summarized. A multiple choice test 55 is administered on-line for the end-user relating to subject matter of the license. The end-user's answers are entered and examined for correctness at step 56, wherein a relevant

clarification page 50, 51, 52, 53 corresponding to the license section that pertains to an incorrectly answered question is respectively displayed. The end-user reviews license sections pertaining to incorrectly answered questions and attempts to answer new questions presented in a modified test at step 55 in substantially the same manner described above. If the end-user answers the original or new questions correctly, a license is issued at step 57 and the end-user is permitted to access and download the site copying software. A new test is generated for each end-user to ensure that each end-user has an individual understanding of the agreement. The license may contain any number of sections with corresponding clarification pages and may be granted in substantially the same manner described above. When the end-user is uncertain about the licensing procedure, the end-user can contact the copy protection system provider by electronic mail, fax, telephone or mail. Further, each page displaying a license section includes an electronic mail, chat (i.e., on-line conversation), or audio visual (AV) internet option to facilitate contacting the copy protection system provider.

Referring back to Fig. 8, similar license approval methods can be accomplished via fax at step 20. In particular, the test can be requested from a fax back telephone number and printed at an end-user location. The test includes multiple choice questions wherein the end-user answers the questions on a form received with the test. The form containing end-user answers is returned to the copy protection system center via fax where the test is automatically graded using bar code and optical character recognition (OCR) scanners in conjunction with a computer system containing bar code and OCR software. Alternatively, regular ground mail may be utilized at step 22 to correspond with the copy protection system center. The copy protection system center generates a new test for each end-user to ensure individual end-user understanding of the license.

Another technique that may be implemented to execute the license utilizes telephone coding on touch tone telephones at step 60. Specifically, the end-user obtains the test and text about the license in preprinted form, wherein the test is customized such that the end-user cannot copy answers from another source. The end-user calls the copy protection system center and is prompted to enter, via telephone keypad, a number corresponding to a type of license desired. The license type and serial number is typically present on the copy protection system computer screen, and may be further ascertained via a screen printout. The serial number of the desired license is entered via the telephone keypad, and the end-user is prompted to answer questions from the test. The end-user enters answers to test questions via the telephone keypad wherein the test is automatically graded as described above via a computer system having a conventional device interpreting tones (i.e., digits) entered by the end-user. The license is granted upon correctly answering all of the questions wherein the end-user is given an access code for obviating the licensing procedure and accessing protected web site material. This technique may alternatively be utilized for licensing software and/or other equipment, registering equipment with a manufacturer, or for licenses that are part of an equipment purchase agreement, such as modems, mass storage devices or computer systems. Further, this technique may be employed when the end-user is totally off-line and a license is required to access or download software on-line, or to access equipment.

Referring to Fig. 9, when the end-user enters information indicating that the end-user does not agree to license terms at step 25, the site examination server software examines the access (i.e., permission) table for the protected web site as described above to uncover protected web site objects (i.e., the "Protection Tag" element of the HTML object data structure is set for protected objects) at step 26. If the access table includes

unprotected web site objects, the site examination server software constructs a limited permission table at step 29 and enables an end-user to access unprotected objects at step 31. However, if all web site objects within the access table are protected, then access by the end-user is forbidden at step 27 and the web site visit is terminated.

Upon the end-user entering information indicating that the end-user agrees to license terms at step 25, the licensing software modifies the end-user cookie file at step 58 (i.e., the file containing end-user information associated with the end-user internet browser) to contain the end-user object data structure with the end-user access information (i.e., name and code) described above. This file is utilized to determine whether or not an end-user possesses a license as described above. The end-user determines at step 28 whether or not to obtain local authorized copies of web site material for storage on the end-user computer system. When the end-user desires to obtain local copies, the end-user downloads (e.g., the download is typically accomplished by selecting a download function from a web page) at step 30 the site copying software to the end-user computer system, and the end-user is permitted to access the protected site at step 32.

Upon determining at step 44 (Fig. 7) that the end-user has visited a protected site (i.e., the cookie file is examined as described above), the end-user determines at step 40 whether or not to obtain local copies of protected web site material. If the end-user desires local copies of protected web site material and determines at step 41 that the site copying software is not resident on the end-user computer system, the end-user downloads the site copying software as described above to the end-user computer system at step 42. After the site examination server software determines the end-user possesses a license, the end-user is permitted to access the protected site at step 32. The end-user may automate obtaining local copies of protected web site material by indicating in the end-user browser that

material from a particular web site is to be copied automatically upon visiting that site a predetermined number of times. The end-user browser is typically supplemented with a counter that maintains the number of times a site is visited. The end-user sets a variable within the browser that indicates the number of visits required to automatically copy web site material from a particular site. When the counter reaches the number of visits indicated by the variable, the browser initiates the site copying software (e.g., a plug-in, stand-alone program or third party software) to automatically produce local copies of web site material. The copies are produced provided that the end-user is authorized or licensed to make such copies. Alternatively, web site material may be copied upon end-user request.

Referring to Fig. 10, when a protected web site includes File Transfer Protocol (FTP) services (i.e., services to download data and/or software), the end-user determines at step 33 whether or not to download available data and/or software from the protected web site. If the end-user does not desire to download data and/or software at an FTP site, the visit is terminated at step 39. However, upon the end-user determining to download data and/or software, the site examination server software reminds the end-user of license copying terms at step 34. Further, the protected web site may include additional local terms and conditions for downloading data and/or software, such as terms related to purchase of files and software. The local terms are typically displayed to the end-user via software resident at the server containing the site. When no local terms exist at step 35, the end-user may download data and/or software at step 37 via FTP services, and subsequently terminate the visit at step 39. When the web site includes additional local terms, the end-user determines at step 36 whether or not to agree to the additional local terms. If the end-user enters information indicating that the end-user agrees to additional

local terms, data and/or software is downloaded at step 37 via FTP services, and the visit is terminated at step 39; otherwise data and/or software is not downloaded as indicated at step 38, and the visit is terminated at step 39.

The copy protection software (e.g., the site examination server software, site copying software and licensing software) is implemented in the 'C' programming language, however, the software may be developed in any of a number of high or low level computing languages. Basically, the software includes independent, but related modules. A first module, namely the site examination server software, examines the web site itself and constructs a permission table in accordance with the web site owner's designation of protected web site components as described above. The site examination server software may reside at the copy protection system server, a third party server (i.e., a a licensed copy of the software) containing the protected web site, or on the web site owner computer system (e.g., as a client version of the software). A second module, namely the site copying software, resides on the end-user computer system and functions in conjunction with the site examination server software similar in relation to a client-server application. The site examination server software constructs permission tables that are utilized by the site copying software to determine end-user access rights to protected web site objects as described above for Fig. 2. The site copying software may be implemented in various computer languages, such as 'C', 'C++', or Java. A third module, namely the licensing software, resides on the copy protection system server and grants licenses to end-users to access protected web site material as described above.

The site examination server software examines the web site to ascertain the web site structure (Fig. 4) and identify web site components within web site files as described above. This task can be performed by high level programming languages, such as 'C' or

'C++', and other utility languages that are oriented towards system management input/output tasks (e.g., Perl). Once all components or objects are encountered in a web site, the site examination server software determines, with owner assistance as described above, web site objects requiring copy protection. This calls for building a database or data structure that is well suited for 'C' or 'C++' computer languages. The site examination server software may utilize a data structure to store protection information and/or permission tables as described above, or use a database wherein an object oriented programming language includes calls to the database as part of the object declaration in the software (i.e., the computer instructions representing the calls are merged with the data or structure type as described above). Alternatively, since other computer languages have the ability to make external database calls (e.g., Perl), the site examination server software can be designed in a manner to function in conjunction with an external database, such as SQL, to store protection information and/or permission tables. Further, the site examination server software may be designed in a manner to interface and be initiated from a Java program since Java is platform independent, includes the capabilities described above, and is designed specifically for the Internet. It is to be understood that the copy protection software may be developed in any of the above described or other computer languages by one of ordinary skill in the art based on the functional description and data structures disclosed in the specification and flow charts illustrated in the drawings.

It will be appreciated that the embodiments described above and illustrated in the drawings represent only a few of the many ways of implementing a web site copy protection system and method.

The present invention is not to be limited to copy protection of web sites, but may be utilized for copy protection of various other works, preferably in computer readable

form, in substantially the same manner described above. For example, the system may (e.g., via software) examine computer readable forms of other works (e.g., works associated with or stored in at least one computer file) and protect those works in substantially the same manner described above.

The present invention may be implemented by an end-user's computer system in combination with a web site owner computer system or any quantity of server or host computer systems residing on the web or in communication with the end-user's computer system. The web site owner, server or host computer systems may perform the web site processing and licensing as described above, while the end-user may communicate with the web site owner, server or host computer systems to download and utilize site copying software through a web browser or other software residing on the end-user computer system as described above. The end-user essentially visits the protected web site and/or copy protection system via the web browser on the end-user's computer system or communicates with the web site owner, server or host computer systems via modem or other communication device, and initiates access and/or the licensing procedure wherein access to protected web site components is restricted to licensed or authorized end-users. The server, host and other computer systems may be implemented by any conventional or other processing systems having the capacity and storage to execute the copy protection software (e.g., site examination server software, licensing software and site copying software). The software (e.g., site examination server software, licensing software and site copying software) may be implemented in any suitable computer language enabling the copy protection system to process the web site or other works and facilitate access and/or reproduction of that web site in substantially the same manner described above. Information may be entered into the copy protection system via keyboard, mouse, voice

recognition, touch screen or any other input device. Further, line prompts, dialog boxes and forms may be arranged in any fashion and have any layout or configuration. Moreover, any type of input mechanism may be utilized to retrieve information from an end-user, such as menus, windows or graphical user interfaces (GUI). The data structures, databases and tables may store and arrange any information in any manner, and may be implemented by any data or storage structures or storage devices capable of storing information required for copy protection.

The software logic or algorithms may be arranged in any manner capable of selectively enabling limited access to protected components of web sites or other works in computer readable form. The copy protection system may examine the web site or other works in any fashion capable of determining the structure of the work and the types of works of the work components. The site copying and other software may be delivered to an end-user via any suitable medium, such as CD-ROM, diskette, downloaded from the Internet or a bulletin board (e.g., via carrier signals) or other transfer mechanism. The software (e.g., site examination server software, licensing software and site copying software) may be installed and executed on a computer system in any conventional or other manner (e.g., an install program, copying files, entering an execute command), and may be implemented to be compatible with any operating system. Further, the permission tables may be arranged in any fashion and may be implemented by any data or storage structure or device. Moreover, the code indicating a licensed end-user may be any type of code or other indication of a license, while the protection level designation and other flags may be any number, code or other characters capable of indicating the desired level or status. The license indication may be implemented by storing any indication in any file or at any memory location, or by any other techniques. In addition, web site or other files

containing works may be modified in any manner to indicate protected components, or separate files, tables or other data storage structures may be utilized to indicate protection of work components.

The license terms and any other information may be displayed to an end-user in any fashion wherein the license may include any quantity of clauses. The test or quiz may be administered and graded in any fashion (e.g., automated or manually) wherein the test may include any type (e.g., true/false, multiple choice, etc.) and any quantity of questions. A license may be granted by the copy protection system based on achievement of any desired test score. Further, the copy protection system may enable an end-user to take the test and/or review license terms in any sequence.

From the foregoing description it will be appreciated that the invention makes available a novel web site copy protection system and method wherein the system selectively enables access and reproduction of protected web sites or other works in computer readable form to licensed or authorized end-users.

Having described preferred embodiments of a new and improved web site copy protection system and method, it is believed that other modifications, variations and changes will be suggested to those skilled in the art in view of the teachings set forth herein. It is therefore to be understood that all such variations, modifications and changes are believed to fall within the scope of the present invention as defined by the appended claims.

WHAT IS CLAIMED IS:

1. A computer system for protecting a work in computer readable form from unauthorized access and/or reproduction, said computer system comprising:

input means for facilitating user entry of information associated with the work;

examination means for retrieving the work in computer readable form based on the entered information and examining the work to identify individual work components contained within the work;

work selection means for facilitating user selection of identified work components for protection;

licensing means for granting licenses to enable end-users to access and/or reproduce work components selected for protection;

permission means for storing authorized access information and information associated with a protection status for each work component, wherein the authorized access information relates to licenses granted by said licensing means; and

access means for determining, based on the authorized access information, the presence of a license granted by said licensing means to an end-user and selectively permitting that end-user to access and/or reproduce work components in response to said license determination and the protection status information stored in said permission means.

2. The computer system of claim 1 wherein the work includes a web site.

3. The computer system of claim 1 wherein said licensing means includes:

license display means for displaying license terms to an end-user;

clarifying means for explaining license terms displayed by said license display means in response to an indication that the end-user does not understand a displayed license term;

test means for administering a test having test questions to the end-user relating to license terms displayed by said license display means; and

license grant means for granting a license to enable the end-user to access and/or reproduce work components selected for protection in response to achieving a passing test score associated with the test.

4. The computer system of claim 3 wherein:

said test means includes:

test question means for administering test questions to an end-user;

answer receiving means for receiving answers to the administered test questions from the end-user;

grading means for determining correctness of the received answers;

answer explaining means for explaining a license term associated with each incorrectly answered test question detected by said grading means;

modified test means for administering a modified test having modified test questions to the end-user relating to license terms in response to the end-user achieving a failing test score associated with the test; and

said license grant means includes:

modified grant means for granting a license to enable the end-user to access and/or reproduce work components selected for protection in response to achieving a passing test score associated with the modified test.

5. The computer system of claim 1 wherein:

said licensing means includes:

code means for associating a code with an end-user in response to said licensing means granting that end-user a license; and

said access means includes:

verification means for determining the presence of a license granted by said licensing means to the end-user by verifying the code associated with the end-user against the authorized access information within said permission means to enable the end-user to access and/or reproduce work components selected for protection in response to verification of the code.

6. The computer system of claim 1 wherein said access means includes:

licensed access means for permitting the end-user to access and/or reproduce work components selected for protection in response to said determination that the end-user has been granted a license by said licensing means; and

unlicensed access means for permitting the end-user to access and/or reproduce only unprotected work components indicated by the protection status information in response to said determination that the end-user has not been granted a license by said licensing means.

7. A program product apparatus having a computer readable medium with computer program logic recorded thereon for facilitating protection of a work in computer

readable form from unauthorized access and/or reproduction, said program product apparatus comprising:

input means for facilitating user entry of information associated with the work;

examination means for retrieving the work in computer readable form based on the entered information and examining the work to identify individual work components contained within the work;

work selection means for facilitating user selection of identified work components for protection;

licensing means for granting licenses to enable end-users to access and/or reproduce work components selected for protection;

permission means for storing authorized access information and information associated with a protection status for each work component, wherein the authorized access information relates to licenses granted by said licensing means; and

access means for determining, based on the authorized access information, the presence of a license granted by said licensing means to an end-user and selectively permitting that end-user to access and/or reproduce work components in response to said license determination and the protection status information stored in said permission means.

8. The apparatus of claim 7 wherein the work includes a web site.

9. A computer data signal embodied in a carrier wave and having computer program logic embedded therein for facilitating protection of a work in computer readable form from unauthorized access and/or reproduction, said computer data signal comprising:

input means for facilitating user entry of information associated with the work;

examination means for retrieving the work in computer readable form based on the entered information and examining the work to identify individual work components contained within the work;

work selection means for facilitating user selection of identified work components for protection;

licensing means for granting licenses to enable end-users to access and/or reproduce work components selected for protection;

permission means for storing authorized access information and information associated with a protection status for each work component, wherein the authorized access information relates to licenses granted by said licensing means; and

access means for determining, based on the authorized access information, the presence of a license granted by said licensing means to an end-user and selectively permitting that end-user to access and/or reproduce work components in response to said license determination and the protection status information stored in said permission means.

10. The computer data signal of claim 9 wherein the work includes a web site.

11. A method for protecting, via a computer system, a work in computer readable form from unauthorized access and/or reproduction, said method comprising the steps of:

(a) entering information associated with the work into the computer system;

(b) retrieving the work in computer readable form, via the computer system, based on the entered information;

(c) examining the work, via the computer system, to identify individual work components contained within the work;

(d) facilitating user selection of identified work components for protection;

(e) granting licenses, via the computer system, to enable end-users to access and/or reproduce work components selected for protection;

(f) storing, via the computer system, authorized access information and information associated with a protection status for each work component, wherein the authorized access information relates to granted licenses;

(g) determining, via the computer system based on the authorized access information, the presence of a license granted to an end-user; and

(h) selectively permitting the end-user to access and/or reproduce work components, via the computer system, in response to said license determination and the protection status information.

12. The method of claim 11 wherein the work includes a web site.

13. The method of claim 11 wherein step (e) further includes:

(e.1) displaying license terms to an end-user;

(e.2) explaining license terms displayed to the end user in response to an indication that the end-user does not understand a displayed license term;

(e.3) administering a test having test questions to the end-user relating to license terms displayed to the end-user; and

(e.4) granting a license to enable the end-user to access and/or reproduce work components selected for protection in response to achieving a passing test score associated with the test.

14. The method of claim 13 wherein:

step (e.3) further includes:

(e.3.1) administering test questions to an end-user;

(e.3.2) receiving answers to the administered test questions from the end-user;

(e.3.3) determining correctness of the received answers;

(e.3.4) explaining a license term associated with each incorrectly answered test question; and

(e.3.5) administering a modified test having modified test questions to the end-user relating to license terms in response to the end-user achieving a failing test score associated with the test; and

step (e.4) further includes:

(e.4.1) granting a license to enable the end-user to access and/or reproduce work components selected for protection in response to achieving a passing test score associated with the modified test.

15. The method of claim 11 wherein:

step (e) further includes:

(e.1) associating a code with an end-user in response to granting that end-user a license; and

step (g) further includes:

(g.1) determining the presence of a license granted to the end-user by verifying the code associated with the end-user against the authorized access information to enable the end-user to access and/or reproduce work components selected for protection in response to verification of the code.

16. The method of claim 11 wherein step (h) further includes:

(h.1) permitting the end-user to access and/or reproduce work components selected for protection in response to said determination that the end-user has been granted a license; and

(h.2) permitting the end-user to access and/or reproduce only unprotected work components indicated by the protection status information in response to said determination that the end-user has not been granted a license.

17. A method for facilitating protection of a work in computer readable form from unauthorized access and/or reproduction, said method comprising the step of:

(a) forming a computer readable medium having computer program logic recorded thereon including input means for facilitating user entry of information associated with the work; examination means for retrieving the work in computer readable form based on the entered information and examining the work to identify individual work components contained within the work; work selection means for facilitating user selection of identified work components for protection; licensing means for granting licenses to enable end-users to access and/or reproduce work components selected for protection; permission means for storing authorized access information and information associated with a protection

status for each work component, wherein the authorized access information relates to licenses granted by said licensing means; and access means for determining, based on the authorized access information, the presence of a license granted by said licensing means to an end-user and selectively permitting that end-user to access and/or reproduce work components in response to said license determination and the protection status information stored in said permission means.

18. The method of claim 17 wherein the work includes a web site.

19. A method for facilitating protection of a work in computer readable form from unauthorized access and/or reproduction, said method comprising the step of:

(a) forming a computer data signal embodied in a carrier wave and having computer program logic embedded therein including input means for facilitating user entry of information associated with the work; examination means for retrieving the work in computer readable form based on the entered information and examining the work to identify individual work components contained within the work; work selection means for facilitating user selection of identified work components for protection; licensing means for granting licenses to enable end-users to access and/or reproduce work components selected for protection; permission means for storing authorized access information and information associated with a protection status for each work component, wherein the authorized access information relates to licenses granted by said licensing means; and access means for determining, based on the authorized access information, the presence of a license granted by said licensing means to an end-user and selectively permitting that

end-user to access and/or reproduce work components in response to said license determination and the protection status information stored in said permission means.

20. The method of claim 19 wherein the work includes a web site.

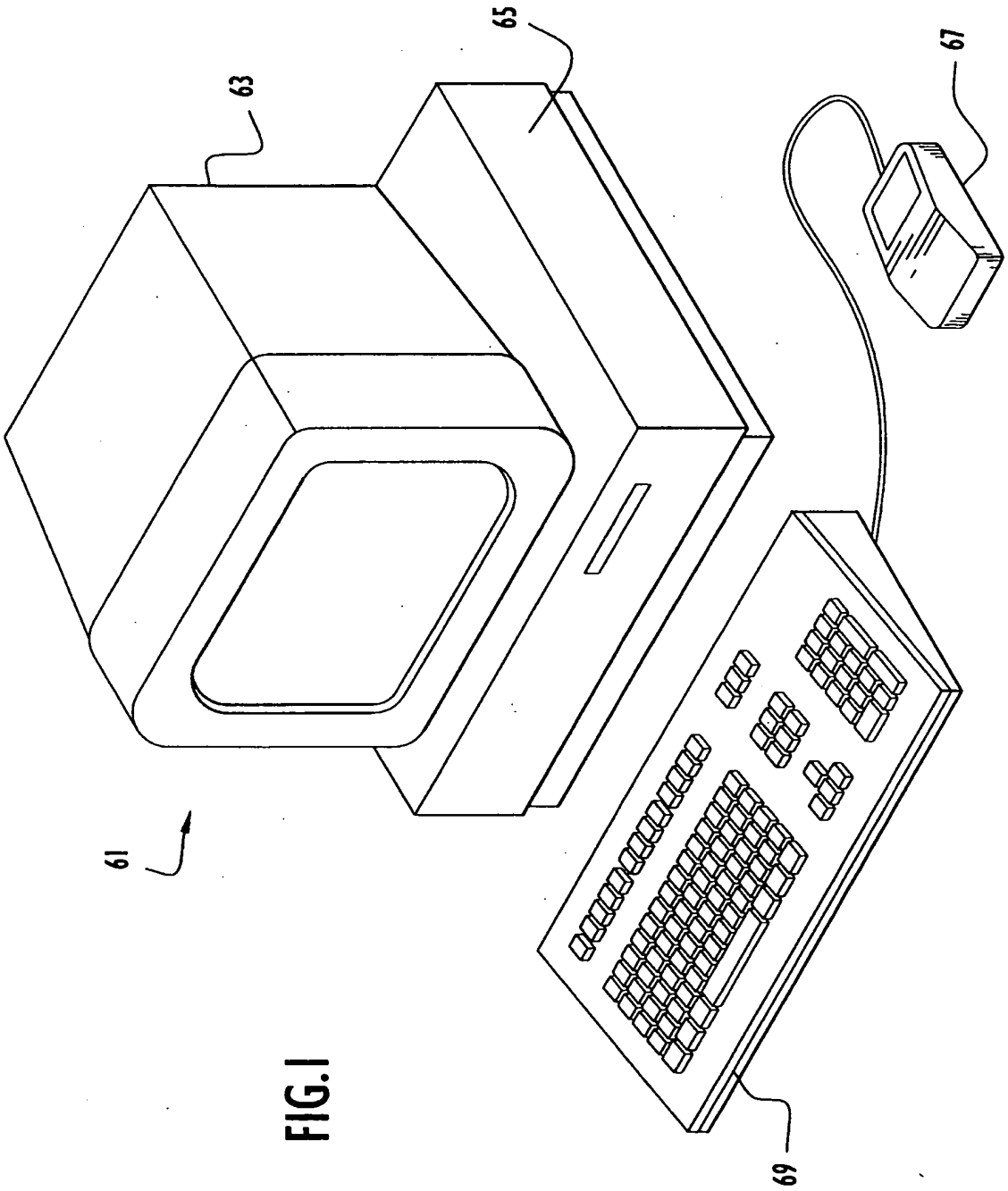


FIG.1

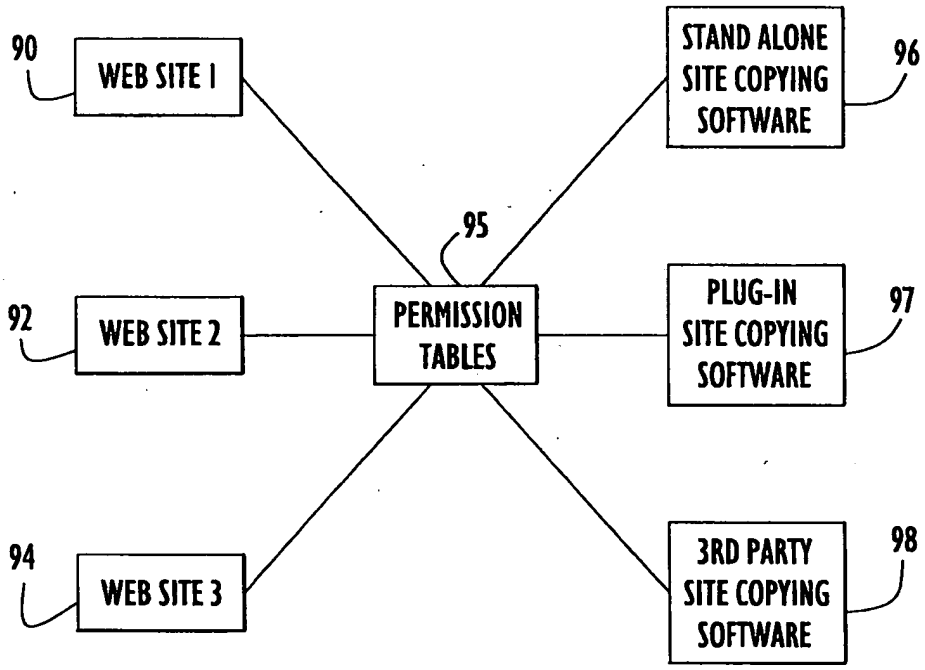

90
WEB SITE 1
92
WEB SITE 2
94
WEB SITE 3
95
PERMISSION TABLES
STAND ALONE SITE COPYING SOFTWARE
96
PLUG-IN SITE COPYING SOFTWARE
97
3RD PARTY SITE COPYING SOFTWARE
98

FIG.2

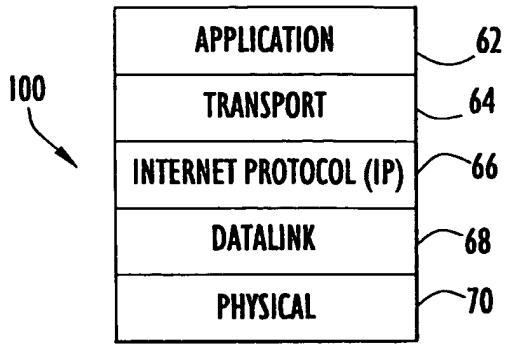
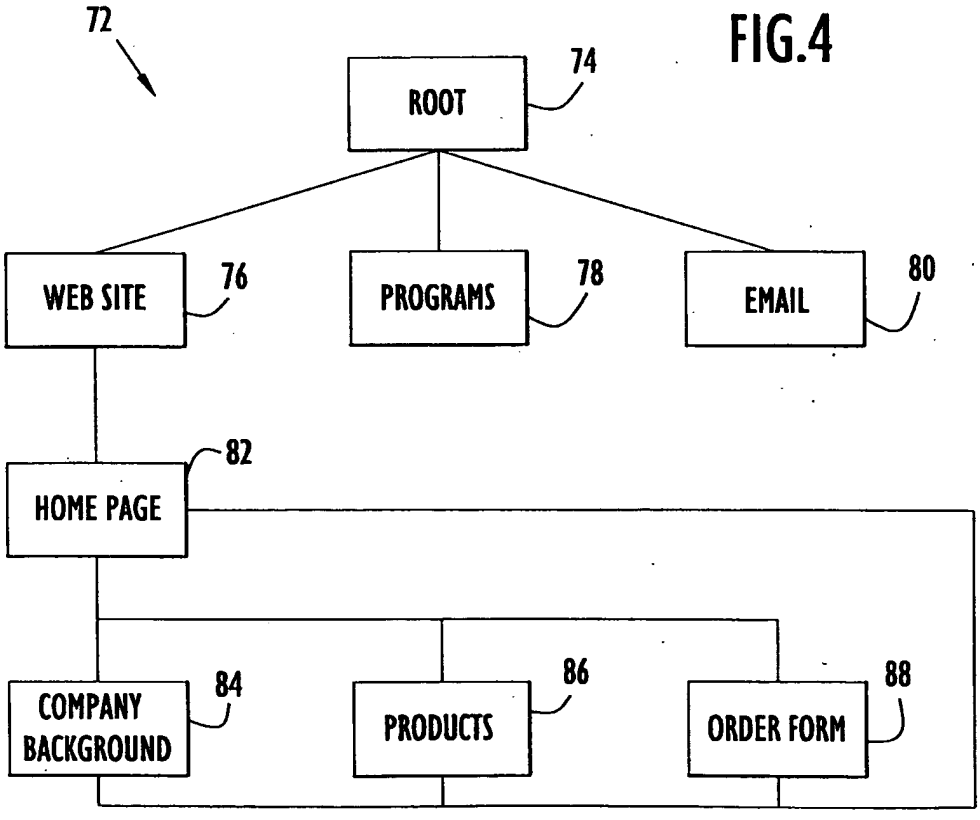

100
APPLICATION
62
TRANSPORT
64
INTERNET PROTOCOL (IP)
66
DATALINK
68
PHYSICAL
70

FIG.3

FIG.4


72
ROOT
74
WEB SITE
76
PROGRAMS
78
EMAIL
80
HOME PAGE
82
COMPANY BACKGROUND
84
PRODUCTS
86
ORDER FORM
88

```
<HTML>
<HEAD>
<TITLE> IMAGE PROTECTION APPLET </TITLE>
</HEAD>
<BODY>
<CENTER> <h1> IMAGE PROTECTION APPLET</h1> </CENTER>
<p>
THE EXAMPLE BELOW SHOWS HOW THE IMAGE PROTECTION APPLET WORKS FOR
IMAGES
BEING IMPLEMENTED VIA MOST SECURE METHOD,NAMELY VIA
AN APPLET.
</p>
<p>
THE IMAGE IS STORED AND TRANSMITTED IN ENCRYPTED FORM,
AND IF IT'S INTERCEPTED,WILL HAVE TO BE DECODED. SPECIAL
PROVISIONS ARE MADE TO PROVIDE (C) NOTICE AND CORRESPONDING
WARNINGS IN THE BODY OF THE IMAGE.
</p>
<p>
ONLY THE APPLET DOWNLOADED FROM THE      SERVERS CAN DECODE
IMAGE AND SHOW IT APPROPRIATELY. WHENEVER USER MOVES TO THE
IMAGE AREA AND/OR CLICKS THERE, HE'LL RECEIVE EXPLICIT (C)
NOTICE IN HIS/HER BROWSER WINDOW.
</p>
<p>
THE APPLET TAKES WIDTH/HEIGHT OF THE IMAGE, BACKGROUND COLOR
AND (C) MESSAGE. IMAGES CAN BE ALIGNED IN FULL ACCORDANCE
WITH APPLET ALIGNMENT TAGS ETC.
</p>
<APPLET CODE="CIMAGE.CLASS" WIDTH=100 HEIGHT=100>
<PARAM NAME=IMAGENAME VALUE=TEST.GIF>
<PARAM NAME=WIDTH VALUE=100>
<PARAM NAME=HEIGHT VALUE=100>
<PARAM NAME=CNOTICE VALUE="THIS IMAGE IS (C) BY      ">
<PARAM NAME=BGCOLOR VALUE=FFFFFF>
</APPLET>
</BODY>
</HTML>
```

FIG.5

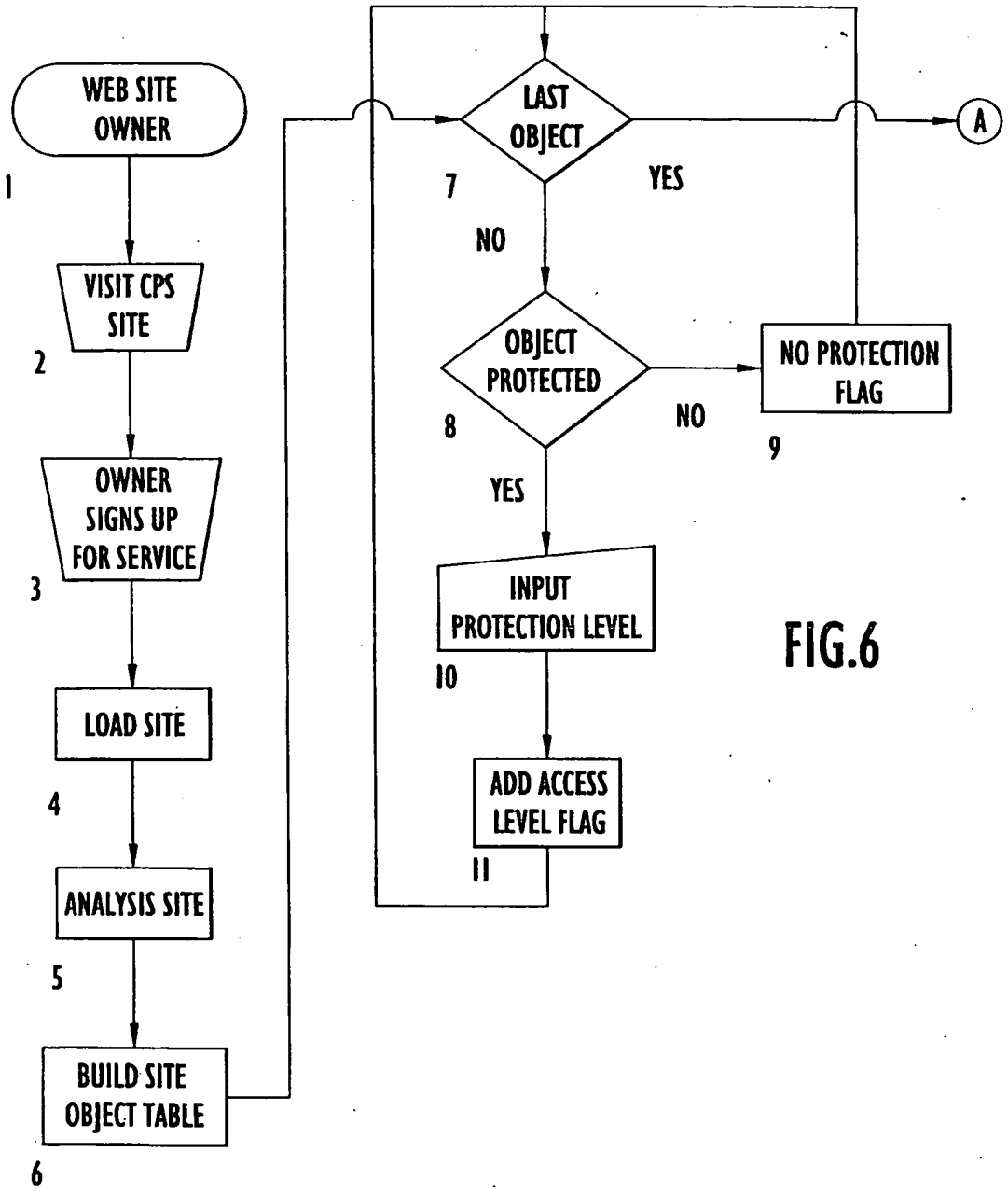

WEB SITE OWNER
1
VISIT CPS SITE
2
OWNER SIGNS UP FOR SERVICE
3
LOAD SITE
4
ANALYSIS SITE
5
BUILD SITE OBJECT TABLE
6
LAST OBJECT
7
YES
NO
OBJECT PROTECTED
8
NO
NO PROTECTION FLAG
9
YES
INPUT PROTECTION LEVEL
10
ADD ACCESS LEVEL FLAG
11
A

FIG.6

FIG.7

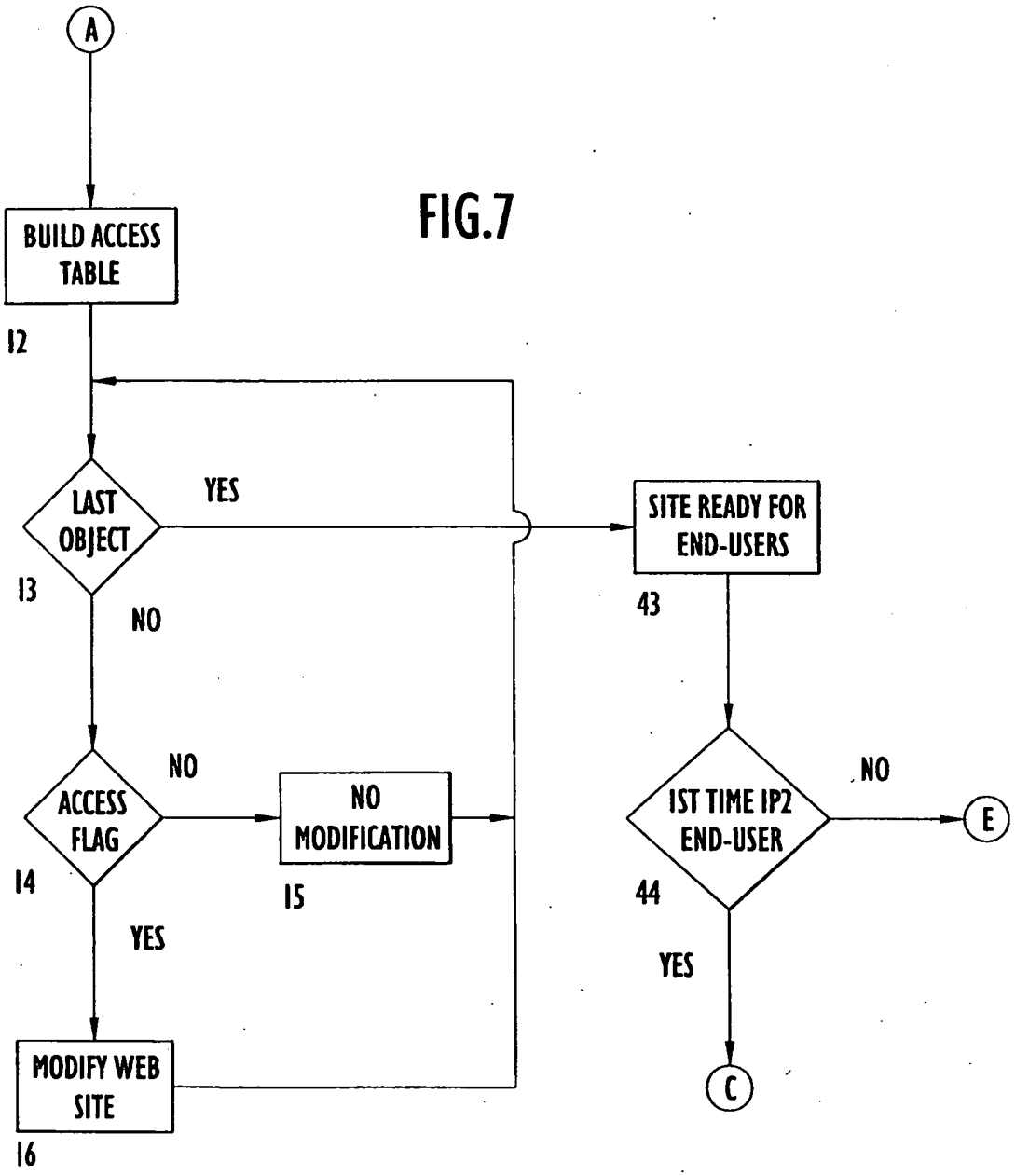

A
BUILD ACCESS TABLE
12
LAST OBJECT
13
YES
NO
SITE READY FOR END-USERS
43
ACCESS FLAG
14
NO
NO MODIFICATION
15
YES
MODIFY WEB SITE
16
1ST TIME IP2 END-USER
44
NO
E
YES
C

FIG.8

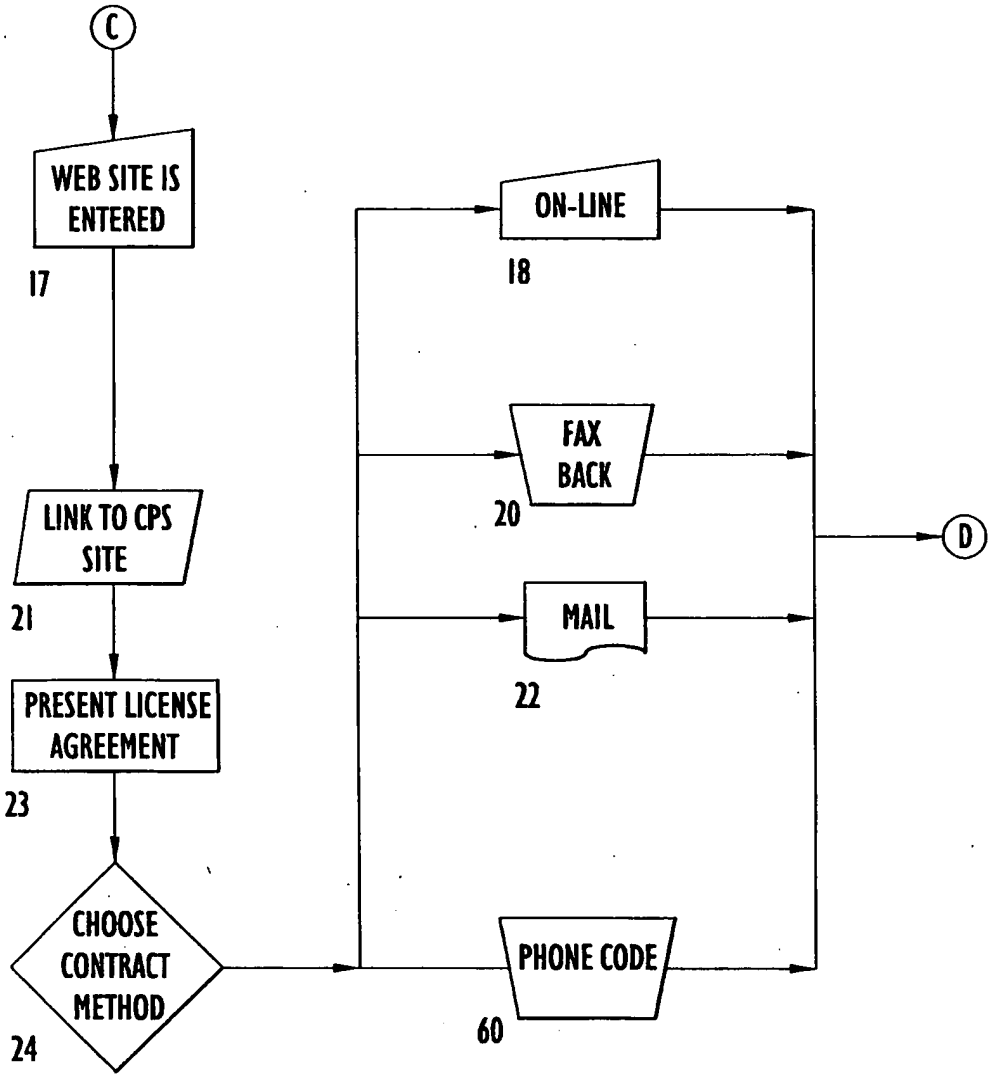

C
WEB SITE IS ENTERED
17
LINK TO CPS SITE
21
PRESENT LICENSE AGREEMENT
23
CHOOSE CONTRACT METHOD
24
ON-LINE
18
FAX BACK
20
MAIL
22
PHONE CODE
60
D

FIG.9

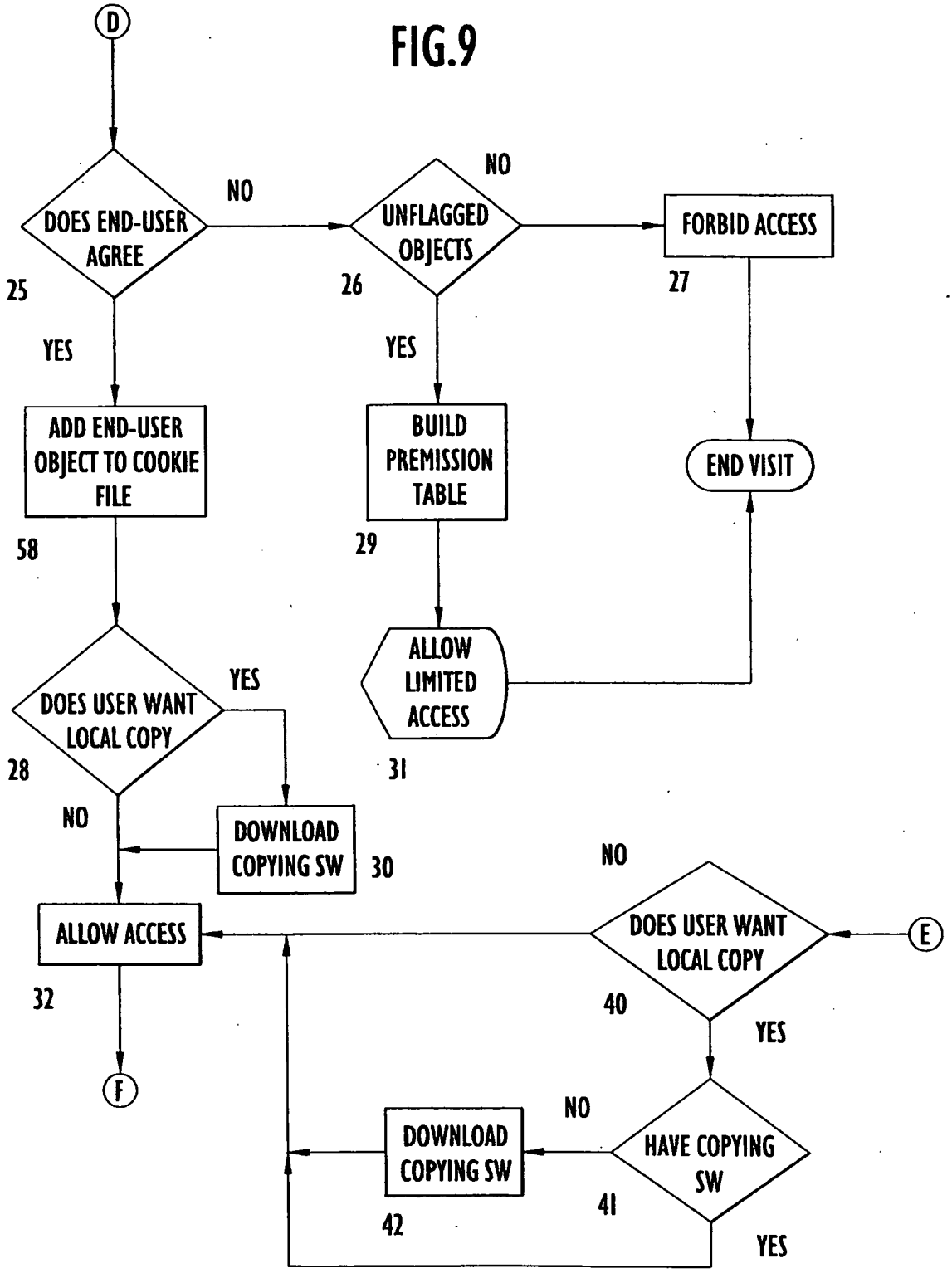
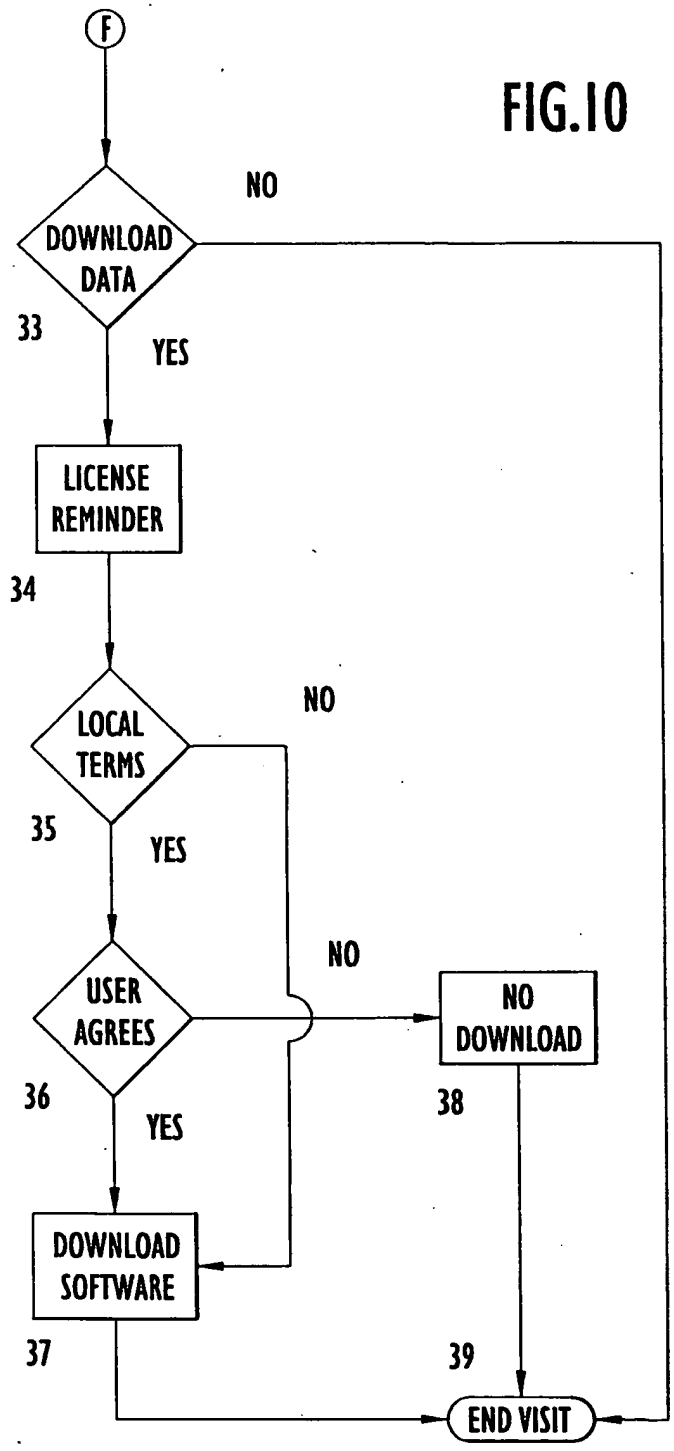

D
DOES END-USER AGREE
25
NO
UNFLAGGED OBJECTS
26
NO
FORBID ACCESS
27
YES
YES
ADD END-USER OBJECT TO COOKIE FILE
58
BUILD PREMISSION TABLE
29
END VISIT
DOES USER WANT LOCAL COPY
28
YES
ALLOW LIMITED ACCESS
31
NO
DOWNLOAD COPYING SW
30
NO
ALLOW ACCESS
32
DOES USER WANT LOCAL COPY
40
E
YES
F
NO
DOWNLOAD COPYING SW
42
HAVE COPYING SW
41
YES

FIG.10


F
DOWNLOAD DATA
NO
33
YES
LICENSE REMINDER
34
LOCAL TERMS
NO
35
YES
USER AGREES
NO
36
YES
NO DOWNLOAD
38
DOWNLOAD SOFTWARE
37
39
END VISIT

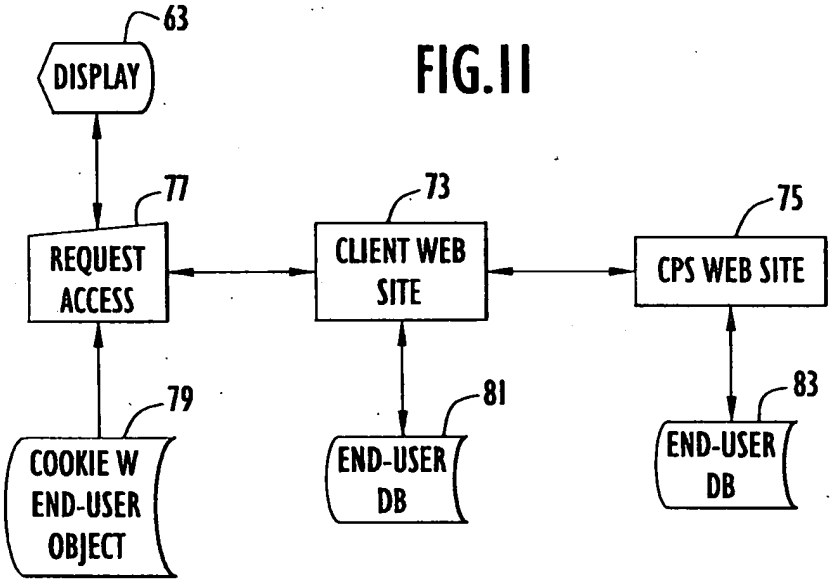
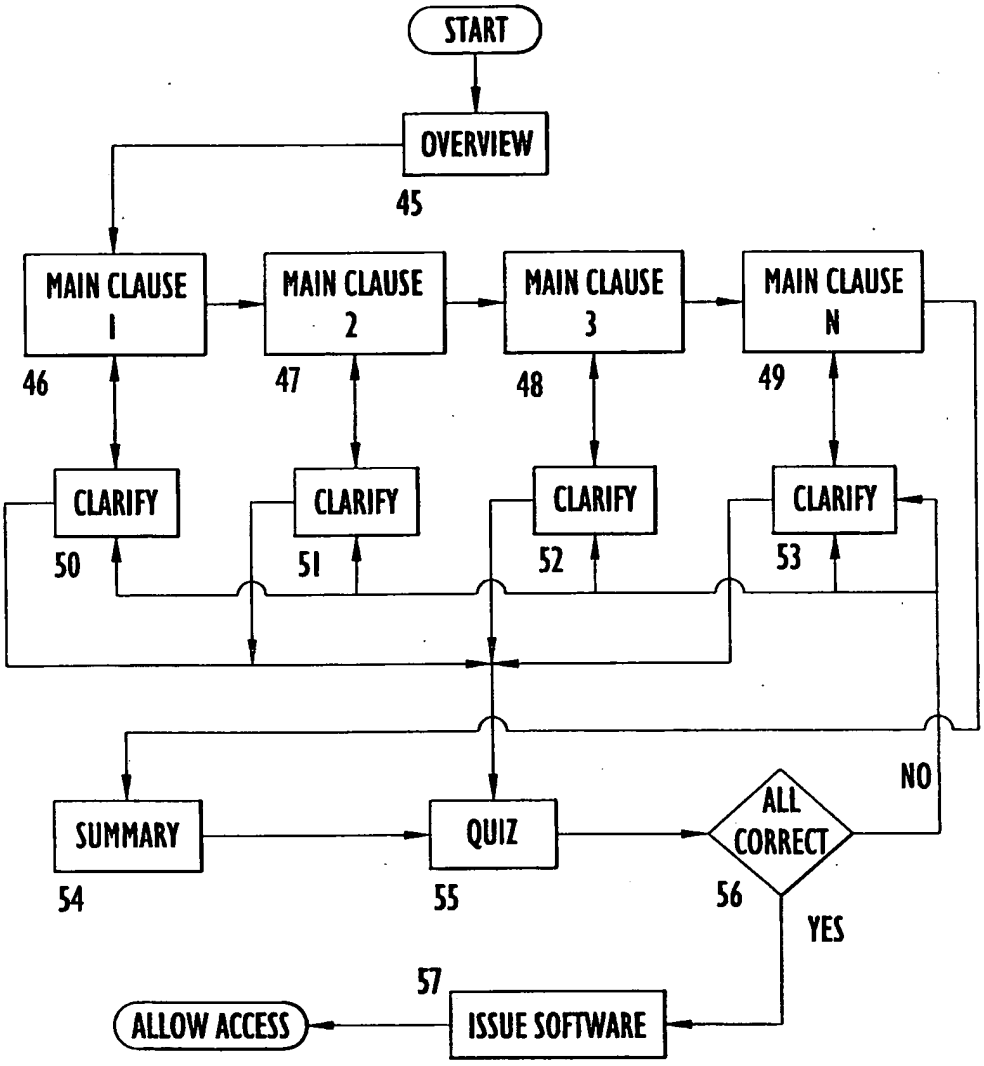

63
DISPLAY
77
REQUEST ACCESS
73
CLIENT WEB SITE
75
CPS WEB SITE
79
COOKIE W END-USER OBJECT
81
END-USER DB
83
END-USER DB

FIG.11

FIG.12


START
OVERVIEW
45
MAIN CLAUSE 1
MAIN CLAUSE 2
MAIN CLAUSE 3
MAIN CLAUSE N
46
47
48
49
CLARIFY
CLARIFY
CLARIFY
CLARIFY
50
51
52
53
SUMMARY
QUIZ
ALL CORRECT
NO
54
55
56
YES
57
ISSUE SOFTWARE
ALLOW ACCESS